What is Claimed:

1. A method for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, comprising:

accepting user input from a user input device;

determining whether said user input is intended for said secured execution environment;

if said user input is not intended for said secured execution environment, transferring said user input to said second execution environment.

2. The method of claim 1, where said step of accepting user input from a user input device comprises decrypting said user input.

3. The method of claim 1, where said step of accepting user input from a user input device comprises establishing a secure communications channel with said user input.

4. The method of claim 1, where said step of accepting user input from a user input device comprises verifying said user input.

5. The method of claim 1, further comprising:

if said user input is intended for said secured execution environment, determining a specific destination entity in said secured execution environment for said user input; and

transferring said user input to said specific destination entity.

6. The method of claim 5, where said step of determining a specific destination entity in said secured execution environment further comprises:

providing window management functionality for managing at least one graphical user interface element owned by said specific destination entity; and

determining that said user input relates to said graphical user interface element.

7. The method of claim 5, where said step of transferring said user input to said specific destination entity comprises:

interpreting said user input.

8. The method of claim 1, further comprising:

accepting output from a specific source entity in said secured execution environment; and

securely transferring said output to an output device.

9. The method of claim 8, where said step of securely transferring said output to said output device comprises:

encrypting said output data.

10. The method of claim 8, where said step of securely transferring said output to said output device comprises:

transferring said output to a curtained memory.

11. A method for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, comprising:

accepting output from a specific source entity in said secured execution environment; and

securely transferring said output to an output device.

12. The method of claim 11, where said step of securely transferring said output to said output device comprises:

encrypting said output data.

13. The method of claim 11, where said step of securely transferring said output to said output device comprises:

transferring said output to a curtained memory.

14. A computer-readable medium containing computer executable instructions to providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, the computer-executable instructions to perform acts comprising:

accepting user input from a user input device;

determining whether said user input is intended for said secured execution environment;

if said user input is not intended for said secured execution environment, transferring said user input to said second execution environment.

15. The computer-readable medium of claim 14, where said accepting user input from a user input device comprises decrypting said user input.

16. The computer-readable medium of claim 14, where said accepting user input from a user input device comprises establishing a secure communications channel with said user input.

17. The computer-readable medium of claim 14, where said accepting user input from a user input device comprises verifying said user input.

18. The computer-readable medium of claim 14, wherein the computer-executable instructions are adapted to perform acts further comprising:

if said user input is intended for said secured execution environment, determining a specific destination entity in said secured execution environment for said user input; and

transferring said user input to said specific destination entity.

19. The computer-readable medium of claim 18, where said determining a specific destination entity in said secured execution environment further comprises:

providing window management functionality for managing at least one graphical user interface element owned by said specific destination entity; and

determining that said user input relates to said graphical user interface element.

20. The computer-readable medium of claim 18, where said transferring said user input to said specific destination entity comprises:

interpreting said user input.

21. The computer-readable medium of claim 14, wherein the computer-executable instructions are adapted to perform acts further comprising:

accepting output from a specific source entity in said secured execution environment; and

securely transferring said output to an output device.

22. The computer-readable medium of claim 21, where said securely transferring said output to said output device comprises:

encrypting said output data.

23. The computer-readable medium of claim 21, where said securely transferring said output to said output device comprises:

transferring said output to a curtained memory.

24. A computer-readable medium containing computer executable instructions to providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, the computer-executable instructions to perform acts comprising:

accepting output from a specific source entity in said secured execution

environment; and

securely transferring said output to an output device.

25. The computer-readable medium of claim 24, where said step of securely transferring said output to said output device comprises:

encrypting said output data.

26. The computer-readable medium of claim 24, where said step of securely transferring said output to said output device comprises:

transferring said output to a curtained memory.

27. A trusted user interface engine for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, comprising:

an input trusted service provider accepting user input from a user input device, operably connected to said user device;

a trusted input manager for determining whether said user input is intended for said secured execution environment and, if said user input is not intended for said secured execution environment, transferring said user input to said second execution environment.

28. The trusted user interface engine of claim 27, where said input trusted service provider decrypts said user input.

29. The trusted user interface engine of claim 27, where said input trusted service provider establishes a secure communications channel with said user input.

30. The trusted user interface engine of claim 27, where said input trusted service provider verifies said user input.

31. The trusted user interface engine of claim 27, where said trusted input manager, if said user input is intended for said secured execution environment, determines a

specific destination entity in said secured execution environment for said user input; and where said trusted input manager further transfers said user input to said specific destination entity.

32. The trusted user interface engine of claim 31, further comprising:

a trusted window manager that provides window management functionality for managing at least one graphical user interface element owned by said specific destination entity; and

where said trusted input manager determines that said user input relates to said graphical user interface element.

33. The trusted user interface engine of claim 31, where said trusted input manager interprets said user input for said specific destination entity.

34. The trusted user interface engine of claim 27, further comprising:

a trusted output manager that accepts output from a specific source entity in said secured execution environment; and that securely transfers said output to an output device.

35. The trusted user interface engine of claim 34, where said trusted output manager encrypts said output data.

36. The trusted user interface engine of claim 34, where said trusted output manager transfers said output to a curtained memory.

37. A trusted user interface engine for providing a secure user interface to a secured execution environment on a system comprising said secured execution environment and an second execution environment, comprising:

a trusted output manager that accepts output from a specific source entity in said secured execution environment; and that securely transfers said output to an output device.

38. The trusted user interface engine of claim 37, where said trusted output manager encrypts said output data.

39. The trusted user interface engine of claim 37, where said trusted output manager transfers said output to a curtained memory.

40. The trusted user interface engine of claim 37, where said trusted output manager comprises:

a trusted rendering interface providing rendering said output from said specific source entity; and where said secure transfer is a transfer of said rendered output.